POWER ANALYSIS ON PRESENT LIGHTWEIGHT CIPHER AND HW COUNTERMEASURE

David Hirš
Bachelor Degree Programme (3), FEEC BUT
E-mail: xhirsd00@stud.feec.vutbr.cz

Supervised by: Zdeněk Martinásek
E-mail: martinasek@feec.vutbr.cz

Abstract: Power analysis presents the typical example of successful attacks against trusted cryptographic devices such as smart cards or emebeded devices. Nowadays, the popularity of Internet of Things (IoT) is growing therefore, designers sould implement cryptographic algorithms with countermeasures in order to defend against these types of attacks. The article focus on the implementation of ultra-lightweight block cipher PRESENT that using the hardware randomization as a countermeasures technique.

Keywords: PRESENT, lightweight cipher, IoT, power analysis, hardware randomization

1 ÚVOD

Proudová analýza (Power analysis, PA) představuje úspěšný typ útoku, který je cílen na dnes běžně používaná kryptografická zařízení, studuje proudovou spotřebu v závislosti na jejich činnosti. Výsledkem analýzy jsou senzitivní informace uložené v kryptografickém zařízení např. šifrovací klíč, které může útočník zneužít k realizaci útoku. Proudová analýza je velice populární, protože k její realizaci nepotřebuje útočník žádné specializované zařízení. Z tohoto důvodu by měli být kryptografické algoritmy implementovány s protiopatřeními, které zamezují realizaci proudové analýzy. Jedním z možných protiopatření je znáhodnění provádění operací algoritmu. Cílem článku je realizace proudové analýzy maskované implementace odlehčeného kryptografického algoritmu PRESENT, který je vhodný pro výpočetně omezená zařízení v IoT.

PRESENT je odlehčená bloková šifra, vzniklá roku 2007 především kvůli potřebám šifrovat data i z velmi omezených zařízení. Taková zařízení jsou například RFID (Radio Frequency Identification) a zařízení v síti senzorů, která mají nižší nároky na zabezpečení. PRESENT je příkladem substitučně-permutační sítě. Sestává z 31 rund s 64 bitovou délkou bloků. Klíče mohou být buď 80, nebo 128 bitů dlouhé. Při pohledu zpět na zařízení v síti senzorů, je doporučené využít 80 bitové klíče z důvodu nižších požadavků na úložiště a výpočetní výkon. Každá z 31 rund má implementovanou operaci XOR, pro zavedení rundovního klíče. Další jsou vrstvy lineární bitové permutace a nelineární substituce. Nelineární vrstva využívá jeden čtyřbitový S-box, který je paralelně aplikován 16krát v každé rundě.

2 PROUDOVÁ ANALÝZA

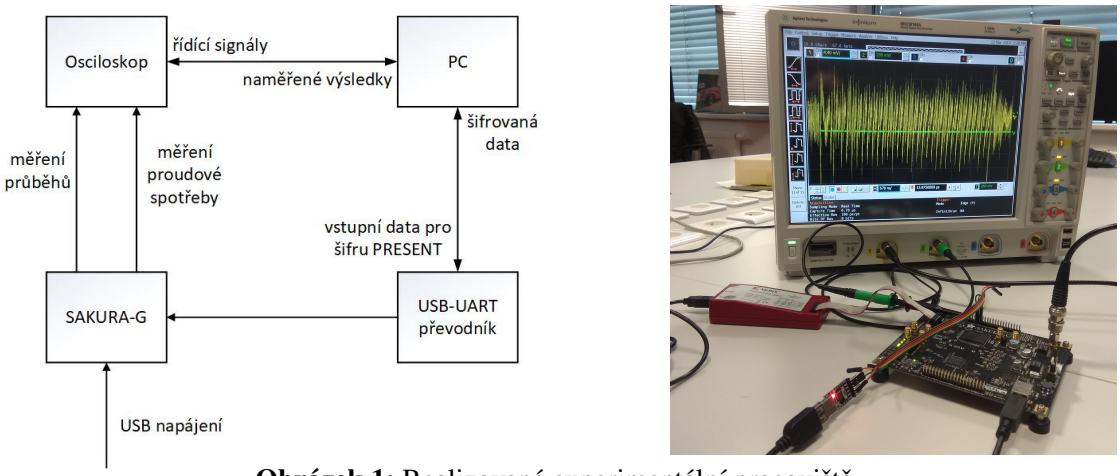
Útoky proudovou analýzou jsou realizovány díky závislosti dynamické proudové spotřeby na právě zpracovávaných datech [1]. Ve většině případů, útočník naměří proudové spotřeby pro náhodná vstupní data (otevřené texty) a poté jsou prodové průběhy vyhodnoceny bez jakéhokoliv invazivního přístupu. Proudová analýza se rozděluje na jednoduchou proudovou analýzu (SPA-Simple Power Analysis) a diferenční proudovou analýzu (DPA-Differential Power Analysis). Jednoduchá proudová analýza využívá malé množství naměřených proudových průběhů. Senzitivní informace je zjištěna přímo z tvaru proudového průběhu.

Diferenční proudová analýza využívá velkého množství naměřených průběhů. DPA nezpracovává proudové průběhy v časové ose, ale analyzuje závislost proudové spotřeby na vstupních datech, v daný časový okamžik. Útok pomocí DPA je realizován v následujících pěti krocích:

- **výběr mezivýsledku implementovaného algoritmu** - Prvním krokem diferenční proudové analýzy je výběr mezivýsledku algoritmu, který je funkcí otevřeného, nebo šifrovaného, textu s tajným klíčem. Mezivýsledkem může být například výstup z funkce S-box nebo AddRoundKey.
- **měření proudové spotřeby** - Druhým krokem je naměření proudové spotřeby při šifrování nebo dešifrování bloků dat. Data musí být útočníkovi během kryptografické operace známá a vždy jiná. Během všech kroků šifrování nebo dešifrování si útočník ukládá naměřené proudové průběhy shodné se zpracovávanými daty.
- **výpočet odhadovaných mezivýsledků** - Ve třetí části útočník vypočítá odhadované mezivýsledky, které jsou hodnoty vstupních dat ve funkci s každou hodnotou tajného klíče.
- **přiřazení odhadovaných mezivýsledků** - Nyní je potřeba přiřadit odhadované mezivýsledky k předpokládaným hodnotám proudové spotřeby. Simulují se proudové spotřeby pomocí modelu Hammingovy váhy, Hammingovy vzdálenosti nebo modelu Zero value. Vybraný model přiřadí každému výsledku odhadovanou hodnotu proudové spotřeby.
- **porovnání odhadovaných mezivýsledků** - Posledním krokem DPA je porovnání odhadovaných mezivýsledků s naměřenými průběhy. Pro porovnání se převážně využívá korelační koeficient. Čím je větší hodnota korelačního koeficientu, tím je správnost odhadovaného výsledku vyšší.

3 VLASTNÍ REALIZACE DPA NA NEMASKOVANÝ ALGORITMUS PRESENT

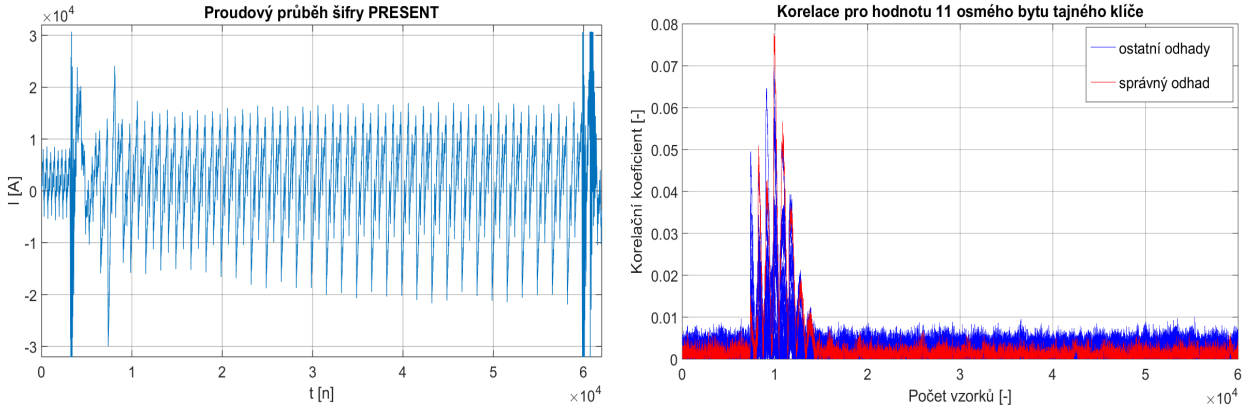
Při realizaci útoku DPA bylo využito pracoviště, jehož podobu zobrazuje obr. 1.



Obrázek 1: Realizované experimentální pracoviště.

Počítač generuje vstupní data pro nemaskovanou šifru PRESENT implementovanou na FPGA (programovatelná hradlová pole) vývojovou desku SAKURA-G a řídící signály pro osciloskop. Komunikace počítače s vývojovou deskou je realizována přes USB se sériovou linku RS-232 na vývojové desce, která je napájená pomocí USB z externího zdroje. Proudová spotřeba je měřena proudovou sondou z osciloskopu na vývojovou desku. Osciloskopem je také měřený počet proudových průběhů. Synchronizace proudové spotřeby je realizována pomocí připojené LED diody s vyvedenými piny pro detekci jejího stavu. Osciloskop dále posílá naměřené hodnoty do počítače pomocí USB rozhraní.

Naměřeno bylo 199 000 proudových průběhů pro různá vstupní data. Útok byl zaměřený na výstup z S-boxové část šifry PRESENT. Po nutných výpočtech a výpočtu korelačního koeficientu byl zjištěný tajný klíč pro každý jednotlivý byte tajného klíče. Graf s nejvyšší hodnotou korelačního koeficientu pro 8. byte tajného klíče znázorňuje obr.2. Tento graf v absolutní hodnotě nám říká, že hodnota pro 8. byte tajného klíče je rovna hodnotě 11, zvýrazněná červeně. Vždy hledáme největší hodnotu nehledě na znaménko. Levý obrázek zobrazuje zmiňovaný proudový průběh. Pro přiřazení odhadovaných mezivýsledků byl použitý model Zero value.



Obrázek 2: Proudový průběh a korelace odhalené hodnoty tajného klíče pro 8. byte

4 PROTIOPATŘENÍ

Implementace protiopatření nezpůsobí odstranění celého postranního kanálu, ale proudová spotřeba je méně závislá na mezivýsledku. Dvěma hlavními skupinami protiopatření jsou *maskování (masking)* a *skrývání (hiding)*. Hardwarové znáhodnění patří do kategorie skrývání. Nele Mentens ve své práci [2] popisuje možnosti rekonfigurace hardwarových zařízení a jejich srovnání na různých hardwarových architekturách. Četně používané hardwarové architektury jsou FPGA. Rekonfigurace FPGA desky poskytuje možnost načtení hardwarových okruhů na vyžádání. Různé skupiny obvodů mohou pracovat na stejném místě FPGA, zároveň však v jiném časovém slotu. Tyto skutečnosti zabraňují útočníkovi v odhadu následujících operací a určení, která operace byla kdy spuštěna nebo provedena. Technika prázdných operací, neboli *dummy operations*, vkládá prázdné operace do prováděného algoritmu, vždy na jiná místa. Při spuštění algoritmu jsou vygenerována umístění, kam se prázdné operace vloží a jejich počet je vždy stejný. Pokud by se počet prázdných operací měnil, útočník by byl schopen zjistit jejich počet opětovným měřením a odečtením časové náročnosti algoritmu. Čím více prázdných operací, tím více se mění jejich umístění v algoritmu a proudová spotřeba je znáhodněná. Počet prázdných operací má však vliv také na časovou náročnost, tedy provedení algoritmu s více prázdnými operacemi je časově mnohem náročnější. Nutností je tedy zvolit mezi rychlostí provedení algoritmu, nebo jeho větším znáhodněním. Druhou technikou je přesouvání prováděných operací, neboli *shuffling of operations*. Některé operace algoritmu není možné přesunout, kvůli jejich návaznosti. Praktické využití je menší, avšak přesouvání operací nemá vliv na časovou náročnost. Hardwarové provedení skýtá možnost náhodně měnit frekvenci hodinového pulzu, vynechat hodinový pulz a přepínat mezi více zdroji hodinového signálu. Metody upravují hodinový signál takovým způsobem, aby nebylo možné synchronizovat proudovou spotřebu. Možnou volbou je zapojení šumových rušiček, které skryjí užitečný signál a jsou rozmístěné v celém obvodu zařízení. V neposlední řadě filtrování proudové spotřeby je účinné protiopatření, ke kterému se využívá spínacích kapacitorů, zdrojů konstantního proudu a prvků regulujících proudovou spotřebu.

Realizovaná DPA prokázala možnost odhalení celého tajného klíče při cílení útoku na funkci S-box. Mnou vybrané protiopatření využívá dynamickou rekonfiguraci určitých bloků desky FPGA. Tato vlastnost umožňuje dynamicky měnit implementovanou tabulka pro funkci S-box uvnitř paměti v průběhu kryptografických operací daného zařízení. Práce [3] popisuje stejné možnosti řešení a je mou předlohou pro realizaci zvoleného protiopatření. Funkce S-box je rozdělená do dvou rekonfigurovatelných funkčních tabulek. První obsahuje náhodné hodnoty substituce a je konfigurována tak, aby provedla zvolenou bijekci. Druhá provedenou bijekci implementuje takovým způsobem, že hodnota výstupu první funkční tabulky je vstupem druhé tabulky a provedená kombinace vede k správné hodnotě S-boxu. Výsledná hodnota S-boxu není ukládaná do registrů pro zvýšení bezpečnosti zařízení. Do registru je pouze ukládaná náhodná hodnota z první funkční tabulky, kterou útočník není schopen odhadnout. Změna konfigurace tabulek je prováděná náhodně během dalšího postupu algoritmu. Pozice dvou různých hodnot první tabulky jsou náhodně měněny. Druhá tabulka je dopočítávána z první tak, aby stále platil vztah uvedený výše. Mé výsledky realizace hardwarového znáhodnění jsou v tuto chvíli pouze dílčí, avšak je to hlavní náplní mé bakalářské práce. Práce bude popisovat praktické provedení s reálnými a mnou realizovanými výsledky, které bude možno brzy prezentovat.

5 ZÁVĚR

Článek prakticky dokázal nebezpečí útoku proudovým kanálem na odlehčenou šifru PRESENT. Tato šifra je pro zařízení s nižšími výpočetními možnostmi vyhovující a s rostoucí popularitou IoT lze předpokládat její četnou implementaci. Realizovaný útok pomocí diferenční proudové analýzy však jednoznačně prokázal možnost zjištění tajného klíče použitého při kryptografických operacích zařízení. Hlavním cílem článku je popsat široké možnosti protiopatření proti proudové analýze spolu s implementací hardwarového znáhodnění, díky kterému vzrůstá jistota bezpečí cenných dat. Výsledky implementace protiopatření jsou zatím jen dílčí, ale možnost zvýšit bezpečnost zařízení tímto způsobem je velmi reálná a proveditelná. Má bakalářská práce již bude obsahovat praktické důkazy a výsledky protiopatření.

REFERENCE

[1] KOCHER, Paul, Joshua JAFFE, Benjamin JUN a Pankaj ROHATGI. Introduction to differential power analysis. Journal of Cryptographic Engineering [online]. 2011, 1(1), 5-27 [cit. 2019-2-14]. DOI: 10.1007/s13389-011-0006-y. ISSN 2190-8508.

[2] MENTENS, Nele. Hiding side-channel leakage through hardware randomization: A comprehensive overview. In: 2017 International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS) [online]. IEEE, 2017, 2017, s. 269-272 [cit. 2019-2-15]. DOI: 10.1109/SAMOS.2017.8344639. ISBN 978-1-5386-3437-0.

[3] SASDRICH, Pascal, Amir MORADI, Oliver MISCHKE a Tim GUNEYSU. Achieving side-channel protection with dynamic logic reconfiguration on modern FPGAs. In: 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) [online]. IEEE, 2015, 2015, s. 130-136. ISBN 978-1-4673-7421-7.

[4] BOGDANOV, A., L. R. KNUDSEN, G. LEANDER, C. PAAR, A. POSCHMANN, M. J. B. ROBSHAW, Y. SEURIN a C. VIKKELSOE. PRESENT: An Ultra-Lightweight Block Cipher. PAILLIER, Pascal a Ingrid VERBAUWHEDE, ed. Cryptographic Hardware and Embedded Systems - CHES 2007 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, s. 450-466. Lecture Notes in Computer Science. DOI: 10.1007/978-3-540-74735-2_31. ISBN 978-3-540-74734-5.